

WLAN 系统、无线通信方法和装置

- 5 本申请要求于 2022 年 2 月 24 日提交中国国家知识产权局、申请号为 202210175153.4、申请名称为“WLAN 系统、无线通信方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

- 10 本申请涉及无线通信领域，尤其涉及 WLAN 系统、无线通信方法和装置。

背景技术

- 在无线局域网 (wireless local area networks, WLAN) 中，接入点 (access point, AP) 可以通过单播、组播或广播的方式向站点 (station, STA) 传输报文。为了提高通信的安全性，AP 使用组临时密钥 (group transient key, GTK) 加密组播或广播报文。在 STA 关联 AP 的过程中，STA 从 AP 获取 GTK。STA 使用 GTK 解密组播或广播报文。在实际应用中，为了提高无线信号的覆盖范围，可以通过多个 AP 组成一个 WLAN 系统。

在多个 AP 组成的 WLAN 系统中，每个 STA 只能接收到与自身关联的 AP 的组播或广播报文，导致 AP 的组播或广播通信效率较低。

20

发明内容

本申请提供了一种 WLAN 系统、无线通信方法和装置，通过使用相同的 GTK，第一 AP 可以为第一 STA 和第二 STA 组播或广播第一报文，从而提高第一 AP 的组播或广播通信效率。

- 本申请第一方面提供了一种 WLAN 系统。WLAN 系统包括接入控制器 (access controller, AC)、第一 AP 和第二 AP。第一 AP 和第一 STA 关联。第二 AP 和第二 STA 关联。AC 用于生成第一 GTK，向第一 AP 和第二 AP 发送第一 GTK。第一 AP 用于通过第一 GTK 加密数据，得到第一报文，组播或广播第一报文。第一 AP 用于向第一 STA 发送第一 GTK。第一 GTK 用于第一 STA 根据第一 GTK 解密第一报文。第二 AP 用于向第二 STA 发送第一 GTK。第一 GTK 用于第二 STA 根据第一 GTK 解密第一报文。

- 30 在第一方面的一种可选方式中，AC 用于根据组主密钥 (group master key, GMK)、组随机数和 AC 的介质访问控制 (medium access control, MAC) 地址生成第一 GTK。

- 在第一方面的一种可选方式中，AC 用于向第一 AP 和第二 AP 发送第一消息。第一消息包括第一 GTK。第一消息还包括以下至少一个：第一 AP 和第二 AP 的标识、第一 AP 中的虚拟接入点 (virtual access point, VAP) 的标识、第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、组随机数、完整性群组临时密钥。其中，通过增加前述中的一个或多个内容，可以提高组播或广播的可靠性。例如，第一 AP 根据第一消息中第一 AP 的标识使用第一 GTK。第二 AP 根据第一消息中第二 AP 的标识使用第一 GTK。WLAN 系统中还包括第三 AP。第一消息中不携带第三 AP 的标识。在接收到第一消息后，第三 AP 不使用第一 GTK。AC 还可以生成第二消息。第二消息中携带第二 GTK 和第三 AP 的标识。第三 AP 根据第三 AP 的标识使用第二 GTK。因此，通过增加 AP 的标识，可以提高组播或广播的可靠性。

- 40 在第一方面的一种可选方式中，AC 还用于向第一 AP 和第二 AP 发送第一指示。第一 AP

还用于根据第一指示关闭 GTK 的自动更新。第二 AP 还用于根据第一指示关闭 GTK 的自动更新。当 AC 为第一 AP 时,第一 AP 无需向第一 AP 发送第一指示。第一 AP 向第二 AP 发送第一指示。在本申请中,通过第一指示,可以避免第一 AP 和第二 AP 自动更新第一 GTK,导致第一 AP 和第二 AP 的 GTK 不同。因此,本申请可以提高组播或广播的可靠性。

- 5 在第一方面的一种可选方式中,当存在新的 AP 连接 AC 时,AC 还用于向新的 AP 发送第一消息。当 AC 为第一 AP 时,第一 AP 还用于向新的 AP 发送第一消息。其中,若新的 AP 使用第一 GTK,则第一 AP 可以向新的 AP 关联的 STA 组播或广播第一报文。因此,本申请可以进一步提高组播或广播的通信效率。

- 10 在第一方面的一种可选方式中,当满足以下任意一项条件时,AC 还用于向第一 AP 和第二 AP 发送更新后的第一 GTK。条件包括:AC 重启、AC 中的密钥定时器超时、AC 的加密模式从公开变为加密、使用第一 GTK 的 STA 离线。其中,通过更新第一 GTK,可以提高组播或广播的安全性。

在第一方面的一种可选方式中,AC 还用于根据更新后的 GMK、更新后的组随机数和 AC 的 MAC 地址更新第一 GTK,得到更新后的第一 GTK。

- 15 在第一方面的一种可选方式中,WLAN 系统还包括第三 AP。AC 还用于获取三个 AP 的分组参考信息。三个 AP 包括第一 AP、第二 AP 和第三 AP。AC 还用于根据分组参考信息确定第一 AP 和第二 AP 使用第一 GTK。AC 还用于根据分组参考信息确定第三 AP 使用第二 GTK。第二 GTK 和第一 GTK 不同。其中,WLAN 系统中的多个 AP 之间的距离可能较远。此时,AC 可以根据分组参考信息对多个 AP 进行分组。组内的 AP 使用相同的 GTK,不同组的 AP 使用不同的 GTK。
- 20 因此,本申请可以在提高组播或广播的通信效率的基础上,提高组播或广播的安全性。

- 在第一方面的一种可选方式中,AC 还用于向第三 AP 发送第二 GTK。或,AC 还用于向第三 AP 发送控制指示。第三 AP 用于根据控制指示生成第二 GTK。其中,根据前面的描述可知,AC 可以将多个 AP 进行分组。例如,第一 AP 和第二 AP 属于第一组。第三 AP 属于第二组。对于不同的组,可以存在不同的控制中心。例如,第一组的控制中心可以为 AC。AC 可以为第一 AP 或第二 AP。第二组的控制中心可以为第三 AP。控制中心用于生成和更新本组内的 GTK。因此,通过为不同组分配不同的控制中心,可以降低管理的复杂性。
- 25

- 在第一方面的一种可选方式中,分组参考信息包括 AP 之间的信道质量信息、三个 AP 所关联 STA 的位置信息或三个 AP 所关联 STA 的点播信息。AP 之间的信道质量信息包括三个 AP 中任意两个 AP 之间的信道质量信息。两个 AP 之间的信道质量信息在一定程度上表征了两个 AP 之间的距离。两个 AP 之间的距离在一定程度上表征了一个 AP 关联的 STA 与另一个 AP 之间的信道质量信息。因此,通过 AP 之间的信道质量信息或三个 AP 所关联 STA 的位置信息进行分组,可以提高组播或广播的通信质量。当多个 STA 的点播信息相同时,可以通过一个 AP 为多个 STA 组播或广播点播信息。因此,通过点播信息进行分组,可以提高 AP 的通信效率。
- 30

- 在第一方面的一种可选方式中,第二 STA 还用于从第二 AP 漫游至第一 AP。第一 AP 还用于通过第一 GTK 加密数据,得到第二报文,组播或广播第二报文。第二 STA 还用于根据第一 GTK 解密第二报文。其中,当第一 AP 和第二 AP 使用不同的 GTK,第二 STA 从第二 AP 漫游至第一 AP 后,第一 AP 可能无法及时向第二 STA 发送第一 AP 的 GTK。因此,第二 STA 可能无法正常解密第一 AP 组播或广播的报文。此时,第二 STA 可能会产生异常行为。例如,第二 STA 断开与第一 AP 的关联,重新关联第一 AP。在本申请中,第一 AP 和第二 AP 使用相同的 GTK。
- 35
- 40 因此,即使第一 AP 未及时向第二 STA 发送第一 AP 的 GTK,第二 STA 也可以使用第二 AP 发送的 GTK 解密第一 AP 组播或广播的报文。因此,本申请可以提高组播或广播的可靠性。

在第一方面的一种可选方式中,第一 AP 和第二 AP 使用相同的基本服务集标识符 (basic service set identifier, BSSID)。其中,某些类型的 STA 可能根据 BSSID 只接收关联的 AP 组播或广播的报文。若第一 AP 和第二 AP 的 BSSID 不同,则第二 STA 可能会丢弃第一报文。通过使用相同的 BSSID,可以使得第二 STA 正常接收第一 AP 组播或广播的报文。此时,第一
5 报文中携带的 BSSID 和第二 AP 的 BSSID 相同。因此,本申请可以提高对不同类型的 STA 的兼容性。

在第一方面的一种可选方式中,第一报文为组播报文。第一报文的 IP 地址为第一组播组的 IP 地址。当第一 STA 属于第一组播组时,第一 STA 用于处理解密后的第一报文。当第一 STA 不属于第一组播组时,第一 STA 用于丢弃解密后的第一报文。其中,一个 AP 关联的不同 STA 可以属于不同的组播组。通过 IP 地址划分不同的组播组,可以提高组播的灵活性。类似地,当第二 STA 属于第一组播组时,第二 STA 用于处理解密后的第一报文。当第二 STA 不
10 属于第一组播组时,第二 STA 用于丢弃解密后的第一报文。

在第一方面的一种可选方式中,第二 STA 与第一 AP 之间的信号质量信息大于第一阈值。根据前面的描述可知,本申请可以对 WLAN 系统中的 AP 进行分组。在实际应用中,AC 也可以
15 对 STA 进行分组。例如,当第二 STA 与第一 AP 之间的信号质量信息大于第一阈值时,AC 确定第二 STA 属于第一组播组。当第二 STA 与第一 AP 之间的信号质量信息小于第一阈值时,AC 确定第二 STA 不属于第一组播组。此时,第二 STA 可以接收其它 AP 的组播或广播报文。其它 AP 可以是第二 AP 或第三 AP 等。在本申请中,通过对 STA 进行分组,可以在提高组播或广播通信效率的基础上,提高组播或广播的通信质量。

20 本申请第二方面提供了一种无线通信方法。无线通信方法包括以下步骤:AC 生成第一 GTK。AC 向第一 AP 和第二 AP 发送第一 GTK。第一 GTK 用于第一 STA 和第二 STA 解密第一 AP 组播或广播的第一报文。第一 AP 和第一 STA 关联。第二 AP 和第二 STA 关联。

在第二方面的一种可选方式中,AC 根据 GMK、组随机数和 AC 的 MAC 地址生成第一 GTK。

在第二方面的一种可选方式中,AC 向第一 AP 和第二 AP 发送第一消息。第一消息包括第一 GTK。第一消息还包括以下至少一个:第一 AP 和第二 AP 的标识、第一 AP 中的 VAP 的标识、
25 第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、组随机数或完整性群组临时密钥。

在第二方面的一种可选方式中,无线通信方法还包括以下步骤:AC 向第一 AP 和第二 AP 发送第一指示。第一指示用于第一 AP 和第二 AP 根据第一指示关闭 GTK 的自动更新。

30 在第二方面的一种可选方式中,当满足以下任意一项条件时,无线通信方法还包括以下步骤:AC 向第一 AP 和第二 AP 发送更新后的第一 GTK。条件包括:AC 重启、AC 中的密钥定时器超时、AC 的加密模式从公开变为加密、使用第一 GTK 的 STA 离线。

在第二方面的一种可选方式中,无线通信方法还包括以下步骤:AC 根据更新后的 GMK、更新后的组随机数和 AC 的 MAC 地址更新第一 GTK,得到更新后的第一 GTK。

35 在第二方面的一种可选方式中,在 AC 向第一 AP 和第二 AP 发送第一消息之前,无线通信方法还包括以下步骤:AC 获取三个 AP 的分组参考信息。三个 AP 包括所述第一 AP、第二 AP 和第三 AP。AC 根据分组参考信息确定第一 AP 和第二 AP 使用第一 GTK。AC 根据分组参考信息确定第三 AP 使用第二 GTK。第二 GTK 和第一 GTK 不同。

在第二方面的一种可选方式中,在 AC 根据分组参考信息确定第三 AP 使用第二 GTK 之后,
40 无线通信方法还包括以下步骤:AC 向第三 AP 发送第二 GTK。或,AC 向第三 AP 发送控制指示。控制指示用于第三 AP 根据控制指示生成第二 GTK。

在第二方面的一种可选方式中，分组参考信息包括 AP 之间的信道质量信息、三个 AP 所关联 STA 的位置信息或三个 AP 所关联 STA 的点播信息。其中，AP 之间的信道质量信息包括三个 AP 中任意两个 AP 之间的信道质量信息。

在第二方面的一种可选方式中，在第二 STA 从第二 AP 漫游至第一 AP 后，第一 GTK 还用于第二 STA 根据第一 GTK 解密第一 AP 组播或广播的第二报文。第一 GTK 是第二 STA 从第二 AP 接收到的。

在第二方面的一种可选方式中，第一 AP 和第二 AP 使用相同的 BSSID。

在第二方面的一种可选方式中，第二 STA 与第一 AP 之间的信号质量信息大于第一阈值。

在第二方面的一种可选方式中，当存在新的 AP 连接 AC 时，无线通信方法还包括以下步骤：AC 向新的 AP 发送第一消息。

本申请第三方面提供了一种无线通信方法。无线通信方法包括以下步骤：第一 AP 从 AC 接收第一消息。第一消息包括第一 GTK。第一 AP 通过第一 GTK 加密数据，得到第一报文。第一 AP 组播或广播第一报文。第一 AP 向第一 STA 发送第一 GTK。第一 GTK 用于第一 STA 根据第一 GTK 解密第一报文。第一 AP 和第一 STA 关联。其中，第一 AP 和第二 AP 使用相同的第一 GTK。第一 GTK 用于第二 STA 根据第一 GTK 解密第一报文。第二 STA 和第二 AP 关联。

在第三方面的一种可选方式中，第一消息还包括以下至少一个：第一 AP 和第二 AP 的标识、第一 AP 中的 VAP 的标识、第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、生成第一 GTK 的组随机数或完整性群组临时密钥。

在第三方面的一种可选方式中，无线通信方法还包括以下步骤：第一 AP 接收 AC 发送的第一指示。第一 AP 根据第一指示关闭 GTK 的自动更新。

在第三方面的一种可选方式中，在第二 STA 从第二 AP 漫游至第一 AP 后，无线通信方法还包括以下步骤：第一 AP 通过第一 GTK 加密数据，得到第二报文。第一 AP 组播或广播所述第二报文。第一 GTK 还用于第二 STA 根据第一 GTK 解密第二报文。第一 GTK 是第二 STA 从第二 AP 接收到的。

在第三方面的一种可选方式中，第一 AP 和第二 AP 使用相同的 BSSID。

在第三方面的一种可选方式中，第二 STA 与第一 AP 之间的信号质量信息大于第一阈值。

本申请第四方面提供了一种无线通信方法。无线通信方法包括以下步骤：第一 AP 生成第一 GTK。第一 AP 通过第一 GTK 加密数据，得到第一报文。第一 AP 组播或广播第一报文。第一 AP 向第二 AP 和第一 STA 发送第一 GTK。第一 GTK 用于第一 STA 根据第一 GTK 解密第一报文。第一 AP 和第一 STA 关联。第一 GTK 用于第二 STA 根据第一 GTK 解密第一报文。第二 STA 和第二 AP 关联。

在第四方面的一种可选方式中，第一 AP 生成第一 GTK 包括：第一 AP 根据 GMK、组随机数和第一 AP 的 MAC 地址生成第一 GTK。

在第四方面的一种可选方式中，第一 AP 向第二 AP 和第一 STA 发送第一消息。第一消息包括第一 GTK。第一消息还包括以下至少一个：第二 AP 的标识、第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、生成第一 GTK 的组随机数或完整性群组临时密钥。

在第四方面的一种可选方式中，无线通信方法还包括以下步骤：第一 AP 向第二 AP 发送第一指示。第一指示用于第二 AP 根据第一指示关闭 GTK 的自动更新。

在第四方面的一种可选方式中，在第二 STA 从第二 AP 漫游至第一 AP 后，无线通信方法还包括以下步骤：第一 AP 通过第一 GTK 加密数据，得到第二报文。第一 AP 组播或广播所述第二报文。第一 GTK 还用于第二 STA 根据第一 GTK 解密第二报文。第一 GTK 是第二 STA 从第二 AP 接收到的。

二 AP 接收到的。

在第四方面的一种可选方式中，第一 AP 和第二 AP 使用相同的 BSSID。

在第四方面的一种可选方式中，第二 STA 与第一 AP 之间的信号质量信息大于第一阈值。

本申请第五方面提供了一种无线通信方法。无线通信方法包括以下步骤：第二 AP 生成第一 GTK。第二 AP 向第一 AP 发送第一 GTK。第一 GTK 用于第一 AP 通过第一 GTK 加密数据，得到第一报文。第二 AP 向第二 STA 发送第一 GTK。第一 GTK 用于第二 STA 根据第一 GTK 解密第一 AP 组播或广播的第一报文。第二 STA 和第二 AP 关联。第一 GTK 用于第一 STA 解密第一 AP 组播或广播的第一报文。第一 STA 和第一 AP 关联。

在第五方面的一种可选方式中，第二 AP 生成第一 GTK 包括：第二 AP 根据 GMK、组随机数和第二 AP 的 MAC 地址生成第一 GTK。

在第五方面的一种可选方式中，第二 AP 向第一 AP 发送第一消息。第一消息包括第一 GTK。第一消息还包括以下至少一个：第一 AP 的标识、第一 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、生成第一 GTK 的组随机数或完整性群组临时密钥。

在第五方面的一种可选方式中，无线通信方法还包括以下步骤：第二 AP 向第一 AP 发送第一指示。第一指示用于第一 AP 根据第一指示关闭 GTK 的自动更新。

在第五方面的一种可选方式中，第一 AP 和第二 AP 使用相同的 BSSID。

本申请第六方面提供了一种无线通信装置。无线通信装置可以是 AC。无线通信装置包括生成模块和发送模块。生成模块用于生成第一 GTK。发送模块用于向第一 AP 和第二 AP 发送第一消息。第一消息包括第一 GTK。第一 GTK 用于第一 STA 和第二 STA 解密第一 AP 组播或广播的第一报文。第一 AP 和第一 STA 关联。第二 AP 和第二 STA 关联。

在第六方面的一种可选方式中，生成模块用于根据 GMK、组随机数和无线通信装置的 MAC 地址生成第一 GTK。

在第六方面的一种可选方式中，第一消息还包括以下至少一个：第一 AP 和第二 AP 的标识、第一 AP 中的虚拟接入点 VAP 的标识、第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、组随机数或完整性群组临时密钥。

在第六方面的一种可选方式中，发送模块还用于向第一 AP 和第二 AP 发送第一指示。第一指示用于第一 AP 和第二 AP 根据第一指示关闭 GTK 的自动更新。

在第六方面的一种可选方式中，当满足以下任意一项条件时，发送模块还用于向第一 AP 和第二 AP 发送更新后的第一 GTK；条件包括：无线通信装置重启、无线通信装置中的密钥定时器超时、无线通信装置的加密模式从公开变为加密、使用第一 GTK 的 STA 离线。

在第六方面的一种可选方式中，生成模块还用于根据更新后的 GMK、更新后的组随机数和无线通信装置的 MAC 地址更新第一 GTK，得到更新后的第一 GTK。

在第六方面的一种可选方式中，无线通信装置还包括获取模块和确定模块。获取模块用于获取三个 AP 的分组参考信息。三个 AP 包括第一 AP、第二 AP 和第三 AP。确定模块用于根据分组参考信息确定第一 AP 和第二 AP 使用第一 GTK。确定模块还用于根据分组参考信息确定第三 AP 使用第二 GTK。第二 GTK 和第一 GTK 不同。

在第六方面的一种可选方式中，发送模块还用于向第三 AP 发送第二 GTK。或，发送模块还用于向第三 AP 发送控制指示。控制指示用于第三 AP 根据控制指示生成第二 GTK。

在第六方面的一种可选方式中，分组参考信息包括 AP 之间的信道质量信息、三个 AP 所关联 STA 的位置信息或三个 AP 所关联 STA 的点播信息。其中，AP 之间的信道质量信息包括三个 AP 中任意两个 AP 之间的信道质量信息。

在第六方面的一种可选方式中,在第二 STA 从第二 AP 漫游至第一 AP 后,第一 GTK 还用于第二 STA 根据第一 GTK 解密第一 AP 组播或广播的第二报文。第一 GTK 是第二 STA 从第二 AP 接收到的。

在第六方面的一种可选方式中,第一 AP 和所述第二 AP 使用相同的 BSSID。

5 在第六方面的一种可选方式中,第二 STA 与第一 AP 之间的信号质量信息大于第一阈值。

在第六方面的一种可选方式中,当存在新的 AP 连接无线通信装置时,发送模块还用于向新的 AP 发送第一消息。

本申请第七方面提供了一种无线通信装置。无线通信装置可以是第一 AP。无线通信装置包括接收模块、加密模块和发送模块。接收模块用于从 AC 接收第一消息。第一消息包括第一
10 GTK。加密模块用于通过第一 GTK 加密数据,得到第一报文。发送模块用于组播或广播第一报文。发送模块还用于向第二 AP 和第一 STA 发送第一 GTK。第一 GTK 用于第一 STA 根据第一 GTK 解密第一报文。无线通信装置和第一 STA 关联。第一 GTK 用于第二 STA 根据第一 GTK 解密第一报文。第二 STA 和第二 AP 关联。

在第七方面的一种可选方式中,第一消息还包括以下至少一个:第一 AP 和第二 AP 的标识、第一 AP 中的 VAP 的标识、第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、生成第一 GTK 的组随机数或完整性群组临时密钥。
15

在第七方面的一种可选方式中,无线通信装置还包括关闭模块。接收模块还用于接收 AC 发送的第一指示。关闭模块用于根据第一指示关闭 GTK 的自动更新。

在第七方面的一种可选方式中,在第二 STA 从第二 AP 漫游至第一 AP 后,加密模块还用于通过第一 GTK 加密数据,得到第二报文。发送模块还用于组播或广播第二报文。其中,第一 GTK 还用于第二 STA 根据第一 GTK 解密第二报文。第一 GTK 是第二 STA 从第二 AP 接收到的。
20

在第七方面的一种可选方式中,无线通信装置和第二 AP 使用相同的 BSSID。

在第七方面的一种可选方式中,第二 STA 与无线通信装置之间的信号质量信息大于第一阈值。

25 本申请第八方面提供了一种无线通信装置。无线通信装置可以是第一 AP。无线通信装置包括生成模块、加密模块和发送模块。生成模块用于生成第一 GTK。加密模块用于通过第一 GTK 加密数据,得到第一报文。发送模块用于组播或广播第一报文。发送模块还用于向第二 AP 和第一 STA 发送第一 GTK。第一 GTK 用于第一 STA 根据第一 GTK 解密第一报文。第一 AP 和第一 STA 关联。第一 GTK 用于第二 STA 根据第一 GTK 解密第一报文。第二 STA 和第二 AP 关联。

30 在第八方面的一种可选方式中,生成模块用于根据 GMK、组随机数和第一 AP 的 MAC 地址生成第一 GTK。

在第八方面的一种可选方式中,发送模块用于向第二 AP 和第一 STA 发送第一消息。第一消息包括第一 GTK。第一消息还包括以下至少一个:第二 AP 的标识、第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、生成第一 GTK 的组随机数或完整性群组临时密钥。

35 在第八方面的一种可选方式中,发送模块还用于向第二 AP 发送第一指示。第一指示用于第二 AP 根据第一指示关闭 GTK 的自动更新。

在第八方面的一种可选方式中,在第二 STA 从第二 AP 漫游至第一 AP 后,加密模块还用于通过第一 GTK 加密数据,得到第二报文。发送模块还用于组播或广播所述第二报文。第一 GTK 还用于第二 STA 根据第一 GTK 解密第二报文。第一 GTK 是第二 STA 从第二 AP 接收到的。

40 在第八方面的一种可选方式中,第一 AP 和第二 AP 使用相同的 BSSID。

在第八方面的一种可选方式中,第二 STA 与第一 AP 之间的信号质量信息大于第一阈值。

本申请第九方面提供了一种无线通信装置。无线通信装置可以是第二 AP。无线通信装置包括生成模块和发送模块。生成模块用于生成第一 GTK。发送模块用于向第一 AP 发送第一 GTK。第一 GTK 用于第一 AP 通过第一 GTK 加密数据,得到第一报文。发送模块还用于向第二 STA 发送第一 GTK。第一 GTK 用于第二 STA 根据第一 GTK 解密第一 AP 组播或广播的第一报文。第二 STA 和第一 AP 关联。第一 GTK 用于第一 STA 解密第一 AP 组播或广播的第一报文。第一 STA 和第一 AP 关联。

在第九方面的一种可选方式中,生成模块用于根据 GMK、组随机数和第二 AP 的 MAC 地址生成第一 GTK。

在第九方面的一种可选方式中,发送模块用于向第一 AP 发送第一消息。第一消息包括第一 GTK。第一消息还包括以下至少一个:第一 AP 的标识、第一 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、生成第一 GTK 的组随机数或完整性群组临时密钥。

在第九方面的一种可选方式中,发送模块还用于向第一 AP 发送第一指示。第一指示用于第一 AP 根据第一指示关闭 GTK 的自动更新。

在第九方面的一种可选方式中,第一 AP 和第二 AP 使用相同的 BSSID。

本申请第十方面提供了一种 AC。AC 包括处理器和收发器。处理器用于生成第一 GTK。收发器用于向第一 AP 和第二 AP 发送第一消息。第一消息包括第一 GTK。第一 GTK 用于第一 STA 和第二 STA 解密第一 AP 组播或广播的第一报文。第一 AP 和第一 STA 关联。第二 AP 和第二 STA 关联。

在第十方面的一种可选方式中,处理器用于根据 GMK、组随机数和无线通信装置的 MAC 地址生成第一 GTK。

在第十方面的一种可选方式中,第一消息还包括以下至少一个:第一 AP 和第二 AP 的标识、第一 AP 中的虚拟接入点 VAP 的标识、第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、组随机数或完整性群组临时密钥。

在第十方面的一种可选方式中,收发器还用于向第一 AP 和第二 AP 发送第一指示。第一指示用于第一 AP 和第二 AP 根据第一指示关闭 GTK 的自动更新。

在第十方面的一种可选方式中,当满足以下任意一项条件时,收发器还用于向第一 AP 和第二 AP 发送更新后的第一 GTK;条件包括:无线通信装置重启、无线通信装置中的密钥定时器超时、无线通信装置的加密模式从公开变为加密、使用第一 GTK 的 STA 离线。

在第十方面的一种可选方式中,处理器还用于根据更新后的 GMK、更新后的组随机数和无线通信装置的 MAC 地址更新第一 GTK,得到更新后的第一 GTK。

在第十方面的一种可选方式中,处理器还用于获取三个 AP 的分组参考信息。三个 AP 包括第一 AP、第二 AP 和第三 AP。处理器还用于根据分组参考信息确定第一 AP 和第二 AP 使用第一 GTK。处理器还用于根据分组参考信息确定第三 AP 使用第二 GTK。第二 GTK 和第一 GTK 不同。

在第十方面的一种可选方式中,收发器还用于向第三 AP 发送第二 GTK。或,收发器还用于向第三 AP 发送控制指示。控制指示用于第三 AP 根据控制指示生成第二 GTK。

在第十方面的一种可选方式中,分组参考信息包括 AP 之间的信道质量信息、三个 AP 所关联 STA 的位置信息或三个 AP 所关联 STA 的点播信息。其中,AP 之间的信道质量信息包括三个 AP 中任意两个 AP 之间的信道质量信息。

在第十方面的一种可选方式中,在第二 STA 从第二 AP 漫游至第一 AP 后,第一 GTK 还用于第二 STA 根据第一 GTK 解密第一 AP 组播或广播的第二报文。第一 GTK 是第二 STA 从第二

AP 接收到的。

在第十方面的一种可选方式中,第一 AP 和所述第二 AP 使用相同的 BSSID。

在第十方面的一种可选方式中,第二 STA 与第一 AP 之间的信号质量信息大于第一阈值。

在第十方面的一种可选方式中,当存在新的 AP 连接无线通信装置时,发送模块还用于向
5 新的 AP 发送第一消息。

本申请第十一方面提供了一种第一 AP。第一 AP 包括处理器和收发器。收发器用于从 AC 接收第一消息。第一消息包括第一 GTK。处理器用于通过第一 GTK 加密数据,得到第一报文。收发器用于组播或广播第一报文。收发器还用于向第一 STA 发送第一 GTK。第一 GTK 用于第一 STA 根据第一 GTK 解密第一报文。第一 AP 和第一 STA 关联;其中,第一 AP 和第二 AP 使用
10 相同的第一 GTK。第一 GTK 用于第二 STA 根据第一 GTK 解密第一报文。第二 STA 和第二 AP 关联。

在第十一方面的一种可选方式中,第一消息还包括以下至少一个:第一 AP 和第二 AP 的标识、第一 AP 中的 VAP 的标识、第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、生成第一 GTK 的组随机数或完整性群组临时密钥。

在第十一方面的一种可选方式中,收发器还用于接收 AC 发送的第一指示。处理器还用于根据第一指示关闭 GTK 的自动更新。

在第十一方面的一种可选方式中,在第二 STA 从第二 AP 漫游至第一 AP 后,处理器还用于通过第一 GTK 加密数据,得到第二报文。收发器还用于组播或广播第二报文。其中,第一 GTK 还用于第二 STA 根据第一 GTK 解密第二报文。第一 GTK 是第二 STA 从第二 AP 接收到的。

在第十一方面的一种可选方式中,第一 AP 和第二 AP 使用相同的 BSSID。

在第十一方面的一种可选方式中,第二 STA 与第一 AP 之间的信号质量信息大于第一阈值。

本申请第十二方面提供了一种第一 AP。第一 AP 包括处理器和收发器。处理器用于生成第一 GTK。处理器用于通过第一 GTK 加密数据,得到第一报文。收发器用于组播或广播第一报文。收发器还用于向第二 AP 和第一 STA 发送第一 GTK。第一 GTK 用于第一 STA 根据第一 GTK 解密第一报文。第一 AP 和第一 STA 关联。第一 GTK 用于第二 STA 根据第一 GTK 解密第一报文。
25 第二 STA 和第二 AP 关联。

在第十二方面的一种可选方式中,处理器用于根据 GMK、组随机数和第一 AP 的 MAC 地址生成第一 GTK。

在第十二方面的一种可选方式中,收发器用于向第二 AP 和第一 STA 发送第一消息。第一消息包括第一 GTK。第一消息还包括以下至少一个:第二 AP 的标识、第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、生成第一 GTK 的组随机数或完整性群组临时密钥。

在第十二方面的一种可选方式中,收发器还用于向第二 AP 发送第一指示。第一指示用于第二 AP 根据第一指示关闭 GTK 的自动更新。

在第十二方面的一种可选方式中,在第二 STA 从第二 AP 漫游至第一 AP 后,处理器还用于通过第一 GTK 加密数据,得到第二报文。收发器还用于组播或广播所述第二报文。第一 GTK 还用于第二 STA 根据第一 GTK 解密第二报文。第一 GTK 是第二 STA 从第二 AP 接收到的。

在第十二方面的一种可选方式中,第一 AP 和第二 AP 使用相同的 BSSID。

在第十二方面的一种可选方式中,第二 STA 与第一 AP 之间的信号质量信息大于第一阈值。

本申请第十三方面提供了一种第二 AP。第二 AP 包括处理器和收发器。处理器用于生成第一 GTK。收发器用于向第一 AP 发送第一 GTK。第一 GTK 用于第一 AP 通过第一 GTK 加密数据,得到第一报文。收发器还用于向第二 STA 发送第一 GTK。第一 GTK 用于第二 STA 根据第一 GTK
40

解密第一 AP 组播或广播的第一报文。第二 STA 和第二 AP 关联。第一 GTK 用于第一 STA 解密第一 AP 组播或广播的第一报文。第一 STA 和第一 AP 关联。

在第十三方面的一种可选方式中，处理器用于根据 GMK、组随机数和第二 AP 的 MAC 地址生成第一 GTK。

- 5 在第十三方面的一种可选方式中，收发器用于向第一 AP 发送第一消息。第一消息包括第一 GTK。第一消息还包括以下至少一个：第一 AP 的标识、第一 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、生成第一 GTK 的组随机数或完整性群组临时密钥。

在第十三方面的一种可选方式中，收发器还用于向第一 AP 发送第一指示。第一指示用于第一 AP 根据第一指示关闭 GTK 的自动更新。

- 10 在第十三方面的一种可选方式中，第一 AP 和第二 AP 使用相同的 BSSID。

本申请第十四方面提供了一种计算机存储介质，其特征在于，所述计算机存储介质中存储有指令，所述指令在计算机上执行时，使得所述计算机执行如第二方面或第二方面任意一种实施方式所述的方法；或使得所述计算机执行如第三方面或第三方面任意一种实施方式所述的方法；或使得所述计算机执行如第四方面或第四方面任意一种实施方式所述的方法；或使得所述计算机执行如第五方面或第五方面任意一种实施方式所述的方法。

- 15 本申请第十五方面提供了一种计算机程序产品，其特征在于，所述计算机程序产品在计算机上执行时，使得所述计算机执行如第二方面或第二方面任意一种实施方式所述的方法；或使得所述计算机执行如第三方面或第三方面任意一种实施方式所述的方法；或使得所述计算机执行如第四方面或第四方面任意一种实施方式所述的方法；或使得所述计算机执行如第五方面或第五方面任意一种实施方式所述的方法。

附图说明

- 图 1 为本申请实施例中提供的 WLAN 系统的第一个结构示意图；
图 2 为本申请实施例中提供的无线通信方法的第一个流程示意图；
25 图 3 为本申请实施例中提供的无线通信方法的第二个流程示意图；
图 4 为本申请实施例中提供的第一消息的结构示意图；
图 5 为本申请实施例中提供的 STA 分组方法的第一个流程示意图；
图 6 为本申请实施例中提供的 STA 分组方法的第二个流程示意图；
图 7 为本申请实施例中提供的无线通信方法的第三个流程示意图；
30 图 8 为本申请实施例中提供的无线通信方法的第四个流程示意图；
图 9 为本申请实施例中提供的 WLAN 系统的第二个结构示意图；
图 10 为本申请实施例中提供的无线通信装置的第一个结构示意图；
图 11 为本申请实施例中提供的无线通信装置的第二个结构示意图；
图 12 为本申请实施例中提供的无线通信设备的结构示意图。

35

具体实施方式

本申请提供了一种 WLAN 系统、无线通信方法和装置，通过使用相同的 GTK，第一 AP 可以为第一 STA 和第二 STA 组播或广播第一报文，从而提高第一 AP 的组播或广播通信效率。

- 40 应理解，本申请中使用的“第一”、“第二”等仅用于区分描述的目的，而不能理解为指示或暗示相对重要性，也不能理解为指示或暗示顺序。另外，为了简明和清楚，本申请多个附图中重复参考编号和/或字母。重复并不表明各种实施例和/或配置之间存在严格的限定关

系。示例性地，本申请附图中的以虚线标识的特征或内容可理解为实施例可选的操作或可选的结构。

本申请中的 WLAN 系统应用于无线通信领域。在无线通信领域中，为了提高无线信号的覆盖范围，可以通过多个 AP 组成一个 WLAN 系统。在多个 AP 组成的 WLAN 系统中，每个 STA 只能接收到与自身关联的 AP 的组播或广播报文，导致 AP 的组播或广播通信效率较低。

为此，本申请提供了一种 WLAN 系统和无线通信方法。图 1 为本申请实施例中提供的 WLAN 系统的第一个结构示意图。如图 1 所示，WLAN 系统包括第一 AP 101 和第二 AP 102。第一 AP 101 和第一 STA 103 关联。第二 AP 102 和第二 STA 104 关联。在实际应用中，WLAN 系统还可以包括 AC 105。AC 105 通过无线或有线的方式和第一 AP 101、第二 AP 102 连接。在图 1 的基础上，图 2 为本申请实施例中提供的无线通信方法的第一个流程示意图。如图 2 所示，无线通信方法包括以下步骤。

在步骤 201 中，第一 AP 向第一 STA 发送第一 GTK。第一 AP 101 可以通过以下公式生成第一 GTK。 $GTK = PRF(GMK + GNonce + MAC(AA))$ 。其中，PRF 是一种伪随机函数 (pseudo random function)。Gnonce 是第一 AP 101 生成的一个组随机数。MAC(AA) 是第一 AP 101 的 BSSID。GMK 是第一 AP 101 根据组播会话密钥 (multicast session key, MSK) 生成的。第一 AP 101 可以在预共享密钥模式 (pre-shared key, PSK) 身份认证的过程中生成 MSK。或者，第一 AP 101 可以从第二 AP 102 接收第一 GTK。当 WLAN 系统还包括 AC 105 时，第一 AP 101 可以从 AC 105 接收第一 GTK。或者，第一 AP 101 可以从 AC 105 接收生成 GTK 的信息。第一 AP 101 根据生成 GTK 的信息生成第一 GTK。生成 GTK 的信息可以包括组随机数、GMK 和 AC 105 的 MAC 地址。第一 AP 101 和第一 STA 103 关联。在获取第一 GTK 后，第一 AP 101 向第一 STA 103 发送第一 GTK。

在步骤 202 中，第二 AP 向第二 STA 传输第一 GTK。当第一 AP 101 生成第一 GTK 时，第二 AP 102 可以从第一 AP 101 接收第一 GTK。或者，第二 AP 102 从第一 AP 101 接收第一 AP 101 生成第一 GTK 的信息。第二 AP 102 根据生成第一 GTK 的信息生成第一 GTK。类似地，当 WLAN 系统还包括 AC 105 时，第二 AP 102 可以从 AC 105 接收第一 GTK 或生成 GTK 的信息。第二 AP 获取和第一 AP 相同的第一 GTK。第一 AP 101 和第一 STA 103 关联。在获取第一 GTK 后，第二 AP 102 向第二 STA 104 发送第一 GTK。应理解，步骤 201 和步骤 202 之间没有严格限定的时序关系。

在步骤 203 中，第一 AP 根据第一 GTK 加密数据，得到第一报文。第一报文为组播报文或广播报文。当第一报文为组播报文时，第一报文的的目的 MAC 地址可以为组播 MAC 地址。组播 MAC 地址包括六个字节。六个字节中的第一个字节的最低位为 1。第一报文的的目的 IP 地址可以为组播网际协议 (internet protocol, IP) 地址。当第一报文为广播报文时，第一报文的的目的 MAC 地址可以为广播 MAC 地址。广播 MAC 地址包括六个字节。六个字节中的每个比特都为 1。第一报文的广播 IP 地址可以为广播 IP 地址。

在步骤 204 中，第一 AP 组播或广播第一报文。

在步骤 205 中，第一 STA 根据第一 GTK 解密第一报文。第一 STA 103 在接收到第一报文后，第一 STA 103 可以读取第一报文中的目的 MAC 地址。当第一报文中的目的 MAC 地址为广播 MAC 地址时，第一 STA 103 根据第一 GTK 解密第一报文。当第一报文中的目的 MAC 地址为组播 MAC 地址时，第一 STA 103 确定自身是否属于组播 MAC 地址对应的组播组。当第一 STA 103 属于组播 MAC 地址对应的组播组时，第一 STA 103 根据第一 GTK 解密第一报文。当第一 STA 103 不属于组播 MAC 地址对应的组播组时，第一 STA 103 可以丢弃第一报文。在解密第一报文后，

第一 STA 103 可以获取第一报文的目的 IP 地址。若当第一报文中的目的 IP 地址为广播 IP 地址时，第一 STA 103 可以处理解密后的第一报文。当第一报文中的目的 IP 地址为组播 IP 地址时，第一 STA 103 确定自身是否属于组播 IP 地址对应的组播组。当第一 STA 103 属于组播 IP 地址对应的组播组时，第一 STA 103 可以处理解密后的第一报文。当第一 STA 103 不属于组播 IP 地址对应的组播组时，第一 STA 103 可以丢弃解密后的第一报文。

在步骤 206 中，第二 STA 根据第一 GTK 解密第一报文。关于步骤 206 的描述可以参考前述步骤 205 中的描述。应理解，步骤 205 和步骤 206 之间没有严格限定的时序关系。

在本申请中，第一 AP 101 和第二 AP 102 使用相同的 GTK。因此，第一 AP 可以为第一 STA 和第二 STA 组播或广播第一报文，从而提高第一 AP 组播或广播的通信效率。

在实际应用中，STA 可能在 WLAN 系统中的多个 AP 之间漫游。例如，在图 2 中，第二 STA 104 可以从第二 AP 102 漫游至第一 AP 101。在第二 STA 104 漫游至第一 AP 101 后，第一 AP 101 通过第一 GTK 加密数据，得到第二报文。第一 AP 101 组播或广播第二报文。第二 STA 104 可以根据从第二 AP 102 接收的第一 GTK 解密第二报文。

在实际应用中，第一 AP 101 和第二 AP 102 可以使用相同的 BSSID。第二 STA 104 可以根据相同的 BSSID 确定使用第一 GTK 解密第一报文。应理解，当第一 AP 101 和第二 AP 102 的 BSSID 不同时，第二 AP 102 可以向第二 STA 104 发送指示。指示包括第一 AP 101 的 BSSID。第二 STA 104 可以根据指示确定使用第一 GTK 解密第一报文。应理解，当第二 AP 102 存在多个 VAP 时，第一 AP 101 可以和多个 VAP 中的某个 VAP 使用相同的 BSSID。

根据的前面的描述可知，第一 AP 101 和第二 AP 102 可以通过多种方式获取第一 GTK。在后续的实施例中，将以 AC 105 生成第一 GTK 为例进行描述。应理解，在后续的示例中，AC 105 执行的步骤都可以由第一 AP 101 或第二 AP 102 执行。并且，当第一 AP 101 或第二 AP 102 执行 AC 105 执行的步骤时，第一 AP 101 或第二 AP 102 无需执行与自身的信息交互步骤。例如，在图 2 中，第一 AP 101 生成第一 GTK 时，第一 AP 101 无需向第一 AP 101 发送第一 GTK。

第一 AP 101 和第二 AP 102 中可能设置有密钥定时器。在密钥定时器超时后，第一 AP 101 和第二 AP 102 可以各自更新第一 GTK。但是，第一 AP 101 更新后的第一 GTK 和第二 AP 102 更新后的第一 GTK 可能不同，导致第二 STA 104 无法正常解密第一 AP 101 组播或广播的报文。因此，在本申请实施例中，AC 105 可以统一更新第一 GTK。图 3 为本申请实施例中提供的无线通信方法的第二个流程示意图。如图 3 所示，无线通信方法包括以下步骤。

在步骤 301 中，AC 向第一 AP 和第二 AP 发送第一指示。本申请实施例不限定 AC 105 发送第一指示的方式和第一指示的格式。AC 105 可以通过单播、组播或广播的方式发送第一指示。第一指示的格式可以由 AC 105 和 AP 约定。

在步骤 302 中，第一 AP 根据第一指示关闭 GTK 的自动更新。在接收到第一指示后，第一 AP 101 可以关闭更新 GTK 的密钥定时器。或者，第一 AP 101 可以解除密钥定时器超时和更新 GTK 之间的关系。即在密钥定时器超时后，第一 AP 101 不更新 GTK。应理解，在第一 AP 101 包括多个 VAP 时，第一 AP 101 可以只在目标 VAP 中关闭 GTK 的自动更新。目标 VAP 使用第一 GTK。例如，第一 AP 101 包括第一 VAP 和第二 VAP。第一 VAP 使用第一 GTK。第二 VAP 使用第三 GTK。第一 AP 101 可以只在第一 VAP 中关闭 GTK 的自动更新。此时，在密钥定时器超时后，第一 AP 101 仍可以更新第二 VAP 中的 GTK。

在步骤 303 中，第二 AP 根据第一指示关闭 GTK 的自动更新。关于步骤 303 的描述，可以参考前述步骤 302 中的描述。应理解，步骤 302 和步骤 303 之间没有严格的时序限定。

在步骤 304 中，AC 向第一 AP 和第二 AP 发送第一 GTK。AC 可以根据 GTK、组随机数和 AC

105 的 MAC 地址生成第一 GTK。在生成第一 GTK 后, AC 105 向第一 AP 101 和第二 AP 102 发送第一 GTK。第一 GTK 可以携带在第一消息中。本申请实施例不限定 AC 105 发送第一消息的方式和第一消息的格式。例如, 图 4 为本申请实施例中提供的第一消息的结构示意图。如图 4 所示, 第一消息 401 包括协议版本信息字段、消息类型字段、消息大小字段、AP ID 字段、VAP ID 字段、GTK 字段、密钥重放计数器(replay counter)字段、接收计数器(receive sequence counter, RSC)字段、组随机数(group nonce, Gnonce)字段、完整性群组临时密钥(integrity group transient key, IGTK)字段和保留字段。

协议版本信息字段可以用于指示第一消息是 GTK 同步消息。消息类型字段用于记录第一消息的类型, 例如, 第一消息的类型为控制消息。消息大小字段用于记录第一消息的数据大小。AP ID 字段用于记录使用第一 GTK 的 AP 的标识。例如, 在本申请实施例中, AP ID 字段包括第一 AP 101 和第二 AP 102 的标识。VAP ID 字段记录使用第一 GTK 的 VAP 的标识。例如, 第一 AP 101 中的第一 VAP 使用第一 GTK。此时, VAP ID 字段包括第一 VAP 的标识。GTK 字段用于记录第一 GTK。密钥重放计数器字段用于记录第一 GTK 的序列号。第一 GTK 的序列号用于防止攻击者通过截获密钥交换的数据包进行重放来对系统发起攻击。接收计数器字段中携带 RSC 值。RSC 值可以用于同步重放状态。RSC 值可以通告经历了消息完整性代码(message integrity code, MIC)校验失败的帧的临时密钥完整性协议(temporal key integrity protocol, TKIP)的序号计数器(TKIP sequence counter, TSC)值。第一 AP 101 或第二 AP 102 可以根据 RSC 值识别重放的第一消息。组随机数字段记录了用于生成第一 GTK 的组随机数。完整性群组临时密钥字段携带有校验信息。第一 AP 101 或第二 AP 102 可以根据校验信息校验第一消息的完整性。保留字段也称为预留字段。

在步骤 305 中, AC 更新第一 GTK。AC 105 可以更新 GMK, 以得到更新后的 GMK。AC 105 还可以更新组随机数, 以得到更新后的组随机数。AC 105 根据更新后的 GMK、更新后的组随机数和 AC 105 的 MAC 地址生成更新后的第一 GTK。

在步骤 306 中, AC 向第一 AP 和第二 AP 发送更新后的第一 GTK。当满足以下任意一项或多项条件时, AC 105 向第一 AP 101 和第二 AP 102 发送更新后的第一 GTK。条件包括: AC 105 重启、AC 105 中的密钥定时器超时、AC 105 的加密模式从公开变为加密、使用第一 GTK 的 STA 离线。AC 105 中可以设置有密钥定时器, 在密钥定时器超时后, AC 105 向第一 AP 101 和第二 AP 102 发送更新后的第一 GTK。使用第一 GTK 的 STA 可以是与第一 AP 101 或第二 AP 102 关联的 STA。例如, 当第一 STA 103 离线后, AC 105 向第一 AP 101 和第二 AP 102 发送更新后的第一 GTK。

应理解, 更新后的第一 GTK 可以携带在更新后的第一消息中。关于第一消息的描述, 可以参考前述图 4 中的相关描述。在后续的描述中, 关于一个设备向另一个设备发送的 GTK 的描述, 都可以参考本申请实施例对第一消息的描述。

应理解, 在图 3 中, 本申请实施例只是以第一 AP 101 和第二 AP 102 为例进行描述。在实际应用中, WLAN 系统中的更多 AP 可以使用相同的第一 GTK。并且, 当存在新的 AP 连接 AC 105 时, AC 105 可以向新的 AP 发送第一 GTK。

在本申请实施例中, 第一 AP 101 可以向第二 STA 104 组播或广播第一报文。并且, 第二 STA 104 未与第一 AP 101 关联。因此, 第二 STA 104 和第一 AP 101 之间的信道质量信息会影响组播或广播的通信质量。为此, AC 105 可以对应所有的 STA 进行分组, 得到 N 个组。N 个组的数量和 N 个 AP 一一对应。所有的 STA 包括与 N 个 AP 中任意一个 AP 关联的 STA。AP 只向对应的 STA 进行组播或广播。下面以 N 等于二为例进行描述, 二个 AP 包括第一 AP 101 和

第二 AP 102。例如，图 5 为本申请实施例中提供的 STA 分组方法的第一个流程示意图。无线通信方法可以包括 STA 分组方法。如图 5 所示，STA 分组方法包括以下步骤。

在步骤 501 中，AC 从第一 AP 和第二 AP 获取 STA 分组参考信息。STA 分组参考信息可以包括所有的 STA 与 N 个 AP 之间的信道质量信息。例如，在图 5 中，N 个 AP 包括第一 AP 101 5 和第二 AP 102。所有的 STA 包括第一 STA 103、第二 STA 104 和第三 STA。第一 STA 103 和第一 AP 101 关联。第二 STA 104、第三 STA 和第二 AP 102 关联。STA 分组参考信息包括第一 STA 103 与第一 AP 101、第二 AP 102 之间的信道质量信息。STA 分组参考信息还包括第二 STA 104 与第一 AP 101、第二 AP 102 之间的信道质量信息。STA 分组参考信息还包括第三 STA 与第一 AP 101、第二 AP 102 之间的信道质量信息。信道质量信息可以是接收的信号强度指示 10 (received signal strength indication, RSSI)、干扰占空比、或噪声等。

在步骤 502 中，AC 根据 STA 分组参考信息对所有的 STA 进行分组，得到 STA 分组信息。AC 105 可以根据不同的方法对所有的 STA 进行分组。例如，图 6 为本申请实施例中提供的 STA 分组方法的第二个流程示意图。如图 6 所示，STA 分组方法包括以下步骤。

在步骤 5020 中，开始。

15 在步骤 5021 中，AC 对 N 个 AP 进行排序，将第一个 AP 作为当前 AP。例如，AC 105 可以从第一 AP 101 和第二 AP 102 获取负载信息或信道状况信息。AC 105 根据第一 AP 101 和第二 AP 102 的负载或信道状况进行排序。负载信息可以包括空闲占空比。AC 105 可以按照空闲占空比进行降序排列。例如，第一 AP 101 的空闲占空比大于第二 AP 102 的空闲占空比。第一 AP 101 排序在前。AC 105 将第一 AP 101 作为当前 AP。

20 在步骤 5022 中，AC 获取所有的 STA 与当前 AP 的信道质量信息。在前述图 5 的步骤 501 中，AC 105 获取了 STA 分组参考信息。STA 分组参考信息包括所有的 STA 与当前 AP 的信道质量信息。所有的 STA 与当前 AP 的信道质量信息包括第一 AP 101 与第一 STA 103、第二 STA 104、第三 STA 之间的信道质量信息。

在步骤 5023 中，AC 建立当前 STA 与当前 AP 的映射关系，当前 STA 与当前 AP 的信道质量信息大于第一阈值。假设第一 AP 101 与第一 STA 103、第二 STA 104 之间的信道质量信息 25 大于第一阈值。第一 AP 101 与第三 STA 之间的信道质量信息小于或等于第一阈值。此时，当前 STA 包括第一 STA 103 和第二 STA 104。第一 AP 101 和第一 STA 103、第二 STA 104 对应。第一 STA 103 和第二 STA 104 也可以称为第一组播组。

30 在步骤 5024 中，AC 确定是否遍历 N 个 AP。在 N 个 AP 中还包括第二 AP 102。因此，AC 105 确定未遍历 N 个 AP。AC 105 执行步骤 5025。

在步骤 5025 中，AC 将下一个 AP 作为当前 AP。AC 将第二 AP 102 作为当前 AP。

在步骤 5026 中，AC 获取剩余的 STA 与当前 AP 的信道质量信息。在前述图 5 的步骤 501 中，AC 105 获取了 STA 分组参考信息。STA 分组参考信息包括剩余的 STA 与当前 AP 的信道质量信息。剩余的 STA 与当前 AP 的信道质量信息包括第二 AP 102 与第三 STA 的信道质量信息。

35 在步骤 5023 中，AC 建立当前 STA 与当前 AP 的映射关系，当前 STA 与当前 AP 的信道质量信息大于第一阈值。假设第二 AP 102 与第三 STA 的信道质量信息大于第一阈值。此时，当前 STA 包括第三 STA。第二 AP 102 和第三 STA 对应。第三 STA 也可以称为第二组播组。

在步骤 5024 中，AC 确定是否遍历 N 个 AP。AC 确定遍历 N 个 AP。AC 105 执行步骤 5027。

在步骤 5027 中，结束。

40 在步骤 503 中，AC 向第二 AP 发送 STA 的 STA 分组信息。STA 分组信息包括第一组播组的信息和第二组播组的信息。其中，根据前述图 6 的描述可知，第二 STA 104 属于第一组播组。

第三 STA 属于第二组播组。组播组的信息可以是组播组的 IP 地址或组播组的 MAC 地址等。例如,第一组播组的信息为第一组播组的 IP 地址。第二组播组的信息为第二组播组的 IP 地址。

在步骤 504 中,第二 AP 向第二 STA 发送第一组播组的信息。

在步骤 505 中,第二 AP 向第三 STA 发送第二组播组的信息。当第一组播组的信息为第一组播组的 IP 地址,第二组播组的信息为第二组播组的 IP 地址时,第二 AP 102 还向第三 STA 和第二 STA 104 发送第一 GTK。第三 STA 从第二 AP 102 接收组播或广播报文。第三 STA 根据第一 GTK 解密组播或广播报文。组播或广播报文的的目的 IP 地址为第二组播组的 IP 地址。第三 STA 还根据第二组播组的 IP 地址处理解密后的组播或广播报文。第二 STA 104 从第一 AP 101 接收组播或广播报文。第二 STA 104 根据第一 GTK 解密组播或广播报文。组播或广播报文的的目的 IP 地址为第一组播组的 IP 地址。第二 STA 104 还根据第一组播组的 IP 地址处理解密后的组播或广播报文。在第二 STA 104 接收到第二 AP 102 发送的组播或广播报文后,第二 STA 104 可以解密组播或广播报文。但是,由于组播或广播报文的的目的 IP 地址为第二组播组的 IP 地址,第二 STA 104 可以丢弃解密后的组播或广播报文。类似地,在第三 STA 接收到第一 AP 101 发送的组播或广播报文后,第二 STA 104 也可以丢弃解密后的组播或广播报文。

当第一组播组的信息为第一组播组的 MAC 地址,第二组播组的信息为第二组播组的 MAC 地址时,第二 AP 102 发送的组播或广播报文的的目的 MAC 地址为第二组播组的 MAC 地址。第三 STA 从第二 AP 102 接收组播或广播报文。第三 STA 根据第一 GTK 解密组播或广播报文。第一 AP 101 发送的组播或广播报文的的目的 MAC 地址为第一组播组的 MAC 地址。第二 STA 104 从第一 AP 101 接收组播或广播报文。第二 STA 104 根据第一 GTK 解密组播或广播报文。第三 STA 可以根据第一组播组的 MAC 地址丢弃第一 AP 101 发送的组播或广播报文。类似地,第二 STA 104 可以根据第二组播组的 MAC 地址丢弃第二 AP 102 发送的组播或广播报文。

在步骤 506 中,AC 向第一 AP 发送 STA 分组信息。关于步骤 506 的描述,可以参考前述步骤 503 的描述。

在步骤 507 中,第一 AP 向第一 STA 发送第一组播组的信息。

当第一组播组的信息为第一组播组的 IP 地址时,第一 AP 101 还向第一 STA 103 发送第一 GTK。第一 STA 103 从第一 AP 101 接收组播或广播报文。第一 STA 103 根据第一 GTK 解密组播或广播报文。组播或广播报文的的目的 IP 地址为第一组播组的 IP 地址。第一 STA 103 还根据第一组播组的 IP 地址处理解密后的组播或广播报文。在第一 STA 103 接收到第二 AP 102 发送的组播或广播报文后,第一 STA 103 可以根据第一 GTK 解密组播或广播报文。但是,由于第二 AP 102 发送的组播或广播报文的的目的 IP 地址为第二组播组的 IP 地址,第一 STA 103 可以丢弃解密后的组播或广播报文。

当第一组播组的信息为第一组播组的 MAC 地址时,第一 AP 101 还向第一 STA 103 发送第一 GTK。第一 STA 103 从第一 AP 101 接收组播或广播报文。组播或广播报文的的目的 MAC 地址为第一组播组的 MAC 地址。第一 STA 103 根据第一 GTK 解密组播或广播报文。在第一 STA 103 接收到第二 AP 102 发送的组播或广播报文后,由于第二 AP 102 发送的组播或广播报文的的目的 MAC 地址为第二组播组的 MAC 地址,第一 STA 103 可以丢弃第二 AP 102 发送的组播或广播报文。

应理解,在图 5 中,步骤 503 至步骤 507 中的任意两个步骤之间并没有严格限定的时序关系。图 6 中对 STA 的分组只是一个示例。在实际应用中,本领域技术人员可以根据实际情况对 STA 进行分组。

例如,N 个 AP 包括第一 AP 101 和第二 AP 102。所有的 STA 包括第一 STA 103、第二 STA

104 和第三 STA。在步骤 502 中，AC 105 根据 STA 分组信息确定第一 STA 103、第二 STA 104 和第三 STA 属于第一组播组。AC 105 根据 STA 分组信息确定第二组播组没有 STA。此时，第二 AP 102 可以无需发送组播或广播报文。

又例如，N 个 AP 包括第一 AP 101、第二 AP 102 和第三 AP。所有的 STA 包括第一 STA 103、
5 第二 STA 104、第三 STA 和第四 STA。第四 STA 和第三 AP 关联。在步骤 502 中，AC 105 根据 STA 分组信息确定第一 STA 103、第二 STA 104 和第四 STA 属于第一组播组。第一组播组和第一 AP 101 对应。AC 105 根据 STA 分组信息确定第三 STA 属于第二组播组。第二组播组和第二 AP 102 对应。AC 105 根据 STA 分组信息确定第三组播组没有 STA。第三组播组和第三 AP 对应。此时，第一组播组从第一 AP 101 接收组播或广播报文。第二组播组从第二 AP 102 接收组播或广播报文。第三 AP 可以无需发送组播或广播报文。

在前面的描述中，第一 AP 101 和第二 AP 102 使用相同的第一 GTK。在实际应用中，WLAN 系统中的多个 AP 之间的距离可能较远。此时，AC 105 可以根据 AP 分组参考信息对多个 AP 进行分组。AP 分组参考信息简称为分组参考信息。同一组内的 AP 使用相同的 GTK，不同组的 AP 使用不同的 GTK。例如，图 7 为本申请实施例中提供的无线通信方法的第三个流程示意图。
15 如图 7 所示，无线通信方法包括以下步骤。

在步骤 701 中，AC 从第一 AP、第二 AP 和第三 AP 获取分组参考信息。分组参考信息可以是 AP 之间的信道质量信息、三个 AP 所关联 STA 的位置信息或三个 AP 所关联 STA 的点播信息。其中，AP 之间的信道质量信息包括三个 AP 中任意两个 AP 之间的信道质量信息。三个 AP 包括第一 AP 101、第二 AP 102 和第三 AP。三个 AP 所关联 STA 的位置信息可以包括第一 STA 103 和第二 STA 104 的位置信息。三个 AP 所关联 STA 的点播信息可以包括第一 STA 103 和第二 STA 104 的点播信息。

在步骤 702 中，AC 根据分组参考信息确定第一 AP 和第二 AP 使用第一 GTK，根据分组参考信息确定第三 AP 使用第二 GTK。下面以分组参考信息为 AP 之间的信道质量信息为例进行描述。例如，表一为本申请实施例中提供的 AP 之间的信道质量信息矩阵。如表三所示，第一
25 AP 101 测量的与第二 AP 102 之间的信道质量信息为-60。第一 AP 101 测量的与第三 AP 之间的信道质量信息为 NA。类似地，第二 AP 102 测量的与第一 AP 101 之间的信道质量信息为-59。第二 AP 102 测量的与第三 AP 之间的信道质量信息为 NA。

	第一 AP	第二 AP	第三 AP
第一 AP		-60	NA
第二 AP1	-59		NA
第三 AP2	NA	NA	

表一

在表一中，信道质量信息的数值越大表征信道质量信息越好。NA 表征无法接收到对端的信号。AC 105 根据表一将第一 AP 101 和第二 AP 102 作为第一组。AC 105 根据表一将第三 AP 作为第二组。第一组中的 AP 使用第一 GTK。第二组中的 AP 使用第二 GTK。

在步骤 703 中，AC 向第一 AP 和第二 AP 发送第一 GTK。关于步骤 703 的描述，可以参考前述图 2 中步骤 201 和步骤 202 中的描述。在第一 AP 101 和第二 AP 102 接收到第一 GTK 后，第一 AP 101 和第二 AP 102 可以根据第一 GTK 解密第一 AP 101 组播或广播的第一报文。

35 在步骤 704 中，AC 向第三 AP 发送第二 GTK。关于 AC 105 生成第二 GTK 的描述可以参考前述图 2 中 AC 105 生成第一 GTK 的相关描述。第二 GTK 和第一 GTK 不同。在接收到第二 GTK 后，第三 AP 可以向第四 STA 发送第二 GTK。第四 STA 和第三 AP 关联。第三 AP 可以根据第二

GTK 加密数据, 得到组播或广播报文。第四 STA 可以通过第二 GTK 解密组播或广播报文。应理解, 关于第三 AP 和第四 STA 的描述, 可以参考前述第一 AP 和第一 STA 的描述。例如, AC 105 也可以向第三 AP 发送第一指示。第三 AP 根据第一指示关闭 GTK 的自动更新。

在前述图 7 中, AC 105 既作为第一组的控制中心, 也作为第二组的控制中心。控制中心负责维护本组的 GTK。在实际应用中, 不同组的 AP 可以存在不同的控制中心。例如, 图 8 为本申请实施例中提供的无线通信方法的第四个流程示意图。如图 8 所示, 无线通信方法包括以下步骤。

关于步骤 701 至步骤 703 的描述, 可以参考前述图 7 中步骤 701 至步骤 703 中的描述。

在步骤 801 中, AC 向第三 AP 发送控制指示。本申请实施例不限定控制指示的发送方式和控制指示的格式。控制指示的格式可以由第三 AP 和 AC 105 约定。

在步骤 802 中, 第三 AP 根据控制指示生成第二 GTK。在接收到控制指示后, 第三 AP 根据控制指示成为第二组的控制中心。第三 AP 负责维护第二组的第二 GTK。例如, 第三 AP 根据控制指示生成第二 GTK。第三 AP 还可以向第四 STA 发送第二 GTK。第三 AP 还可以根据控制指示更新第二 GTK, 得到更新后的第二 GTK。第三 AP 向第四 STA 发送更新后的第二 GTK。

应理解, 图 7 和图 8 中只是以三个 AP 为例进行示例性的描述。在实际应用中, AC 105 可以根据实际情况对多个 AP 进行不同的分组。例如, WLAN 系统还包括第四 AP。AC 105 根据参考分组信息将第三 AP 和第四 AP 作为第二组。此时, 在图 8 中, 第三 AP 还可以向第四 AP 发送第二 GTK。

图 9 为本申请实施例中提供的 WLAN 系统的第二个结构示意图。如图 9 所示, WLAN 系统包括第一 AP 101、第二 AP 102、第三 AP 901 和第四 AP 902。AP 外的圆形虚线表征 AP 的信号覆盖范围。AP 与 STA 之间的虚线表征关联关系。其中, 第一 AP 101 和 STA1、STA3 关联。第二 AP 102 和 STA2 关联。第三 AP 901 和 STA4、STA6 关联。第四 AP 902 和 STA5 关联。

AP 与 STA 之间的箭头实线表征组播或广播报文的传输方向。其中, AC 105 (图中未示出) 将第一 AP 101 和第二 AP 102 作为第一组。在第一组中, 第一 AP 101 使用第一 GTK 加密数据, 得到第一报文。第一 AP 101 组播或广播第一报文。STA1、STA2 和 STA3 根据第一 GTK 解密第一报文。AC 105 将第三 AP 901 和第四 AP 902 作为第二组。在第二组中, 第三 AP 901 使用第二 GTK 加密数据, 得到组播或广播报文。STA4、STA5 和 STA6 根据第二 GTK 解密第三 AP 901 发送的组播或广播报文。

在图 9 中, AC 105 可以选定第二组中的某个 AP 作为第二组的控制中心。AC 105 可以根据第二组中各个 AP 处理能力、或第二组中各个 AP 和 AC 105 的关联情况来选择控制中心。例如, AC 105 将第二组中处理能力强的 AP 作为控制中心。或者, AC 105 将与 AC 105 之间的节点数量较少的 AP 作为控制中心。例如, 第三 AP 901 和 AC 105 直连, 第四 AP 902 和 AC 105 通过第一 AP 101 相连。此时, AC 105 将第三 AP 901 作为第二组的控制中心。

前面对本申请实施例中提供的无线通信方法和 WLAN 系统进行描述。下面对本申请实施例中提供的无线通信装置进行描述。图 10 为本申请实施例中提供的无线通信装置的第一个结构示意图。如图 10 所示, 无线通信装置 1000 包括生成模块 1001 和发送模块 1002。生成模块 1001 用于生成第一 GTK。发送模块 1002 用于向第一 AP 和第二 AP 发送第一消息。第一消息包括第一 GTK。第一 GTK 用于第一站点 STA 和第二 STA 解密第一 AP 组播或广播的第一报文。第一 AP 和第一 STA 关联。第二 AP 和第二 STA 关联。

应理解, 无线通信装置 1000 可以是前述无线通信方法或 WLAN 系统中的 AC 105。因此, 关于无线通信装置 1000 中的描述, 可以参考前述无线通信方法或 WLAN 系统中的相关描述。

例如,发送模块 1002 还可以用于向第一 AP 发送第一指示。又例如,发送模块 1002 还可以用于向第一 AP 发送更新后的第一 GTK。

图 11 为本申请实施例中提供的无线通信装置的第二个结构示意图。如图 11 所示,无线通信装置 1100 包括生成模块 1101、加密模块 1102 和发送模块 1103。生成模块 1101 用于生成第一 GTK。加密模块 1102 用于通过第一 GTK 加密数据,得到第一报文。发送模块 1103 用于组播或广播所述第一报文。发送模块 1103 还用于向第二 AP 和第一 STA 发送第一 GTK。第一 GTK 用于第一 STA 根据第一 GTK 解密第一报文。无线通信装置 1100 和第一 STA 关联。第一 GTK 用于第二 STA 根据第一 GTK 解密第一报文。第二 STA 和所述第二 AP 关联。

应理解,无线通信装置 1100 可以是前述无线通信方法或 WLAN 系统中的第一 AP 101。因此,关于无线通信装置 1100 中的描述,可以参考前述无线通信方法或 WLAN 系统中的相关描述。例如,加密模块 1102 还可以用于根据第一 GTK 加密数据,得到第二报文。发送模块 1003 还可以用于组播或广播第二报文。又例如,无线通信装置 1100 还可以包括接收模块和关闭模块。接收模块用于从 AC 接收第一指示。关闭模块根据第一指示关闭 GTK 的自动更新。

图 12 为本申请实施例中提供的无线通信设备的结构示意图。如图 12 所示,无线通信设备 1200 包括处理器 1201 和收发器 1202。无线通信设备 1200 可以为 WLAN 系统或无线通信方法中的 AC 或第一 AP。

当无线通信设备 1200 为 AC 时,处理器 1201 用于生成第一 GTK。收发器 1202 用于向第一 AP 和第二 AP 发送第一消息。第一消息包括第一 GTK。第一 GTK 用于第一 STA 和第二 STA 解密第一 AP 组播或广播的第一报文。第一 AP 和第一 STA 关联。第二 AP 和第二 STA 关联。

应理解,关于无线通信设备 1200 的相关描述,可以参考前述无线通信方法或 WLAN 系统中的相关描述。处理器 1201 还可以用于执行前述无线通信方法中 AC 105 所执行的处理步骤。例如,处理器 1201 还可以用于执行图 3 中的步骤 305。又例如,处理器 1201 还可以用于执行图 5 中的步骤 502。收发器 1202 还可以用于执行前述无线通信方法中 AC 105 所执行的发送或接收步骤。例如,收发器 1202 还可以用于图 3 中的步骤 301。又例如,收发器 1202 还可以用于图 5 中的步骤 501 和步骤 503。

当无线通信设备 1200 为第一 AP 时,处理器 1201 用于生成第一 GTK。处理器 1201 用于通过第一 GTK 加密数据,得到第一报文。收发器 1202 用于组播或广播第一报文。收发器 1202 还用于向第二 AP 和第一 STA 发送第一 GTK。第一 GTK 用于第一 STA 根据第一 GTK 解密第一报文。第一 AP 和第一 STA 关联。第一 GTK 用于第二 STA 根据第一 GTK 解密第一报文。第二 STA 和第二 AP 关联。

应理解,关于无线通信设备 1200 的相关描述,可以参考前述无线通信方法或 WLAN 系统中的相关描述。处理器 1201 还可以用于执行前述无线通信方法中第一 AP 101 所执行的处理步骤。例如,处理器 1201 还可以用于执行图 3 中的步骤 302。收发器 1202 还可以用于执行前述无线通信方法中第一 AP 101 所执行的发送或接收步骤。例如,收发器 1202 还可以用于图 5 中的步骤 504。

在其它实施例中,无线通信设备 1200 还可以包括存储器 1203。存储器 1203 可以是非易失性存储器,比如硬盘(hard disk drive, HDD)等,还可以是易失性存储器(volatile memory),例如随机存取存储器(random-access memory, RAM)。存储器 1203 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质,但不限于此。

存储器 1203 可以用于存储第一 GTK 或第一报文。存储器 1203 也可以用于存储指令,以使得处理 1201 可以用于执行如前述无线通信方法中提及的步骤。或者,存储 1203 也可以用于

于存储其他指令，以配置处理器 1201 的参数以实现对应的功能。

应理解，图 12 所述的装置也可以用于执行前述提及的附图所示的实施例变形或者可选方案中所提及的方法步骤，在此不再赘述。

本申请实施例中处理器 1201 可以是通用处理器、数字信号处理器、专用集成电路、现场可编程门阵列或者其他可编程逻辑器件、分立门或晶体管逻辑器件、分立硬件组件，可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件单元组合执行完成。

处理器 1201 用于实现上述无线通信方法所执行的程序代码可以存储在存储器 1203 中。存储器 1203 和处理器 1201 耦合。本申请实施例中的耦合是装置、单元或模块之间的间接耦合或通信连接，可以是电性，机械或其它的形式，用于装置、单元或模块之间的信息交互。处理器 1201 可能和存储器 1203 协同操作。

基于以上实施例，本申请实施例还提供了一种计算机可读存储介质。该存储介质中存储软件程序，该软件程序在被一个或多个处理器读取并执行时可实现上述任意一个或多个实施例提供的方法。所述计算机可读存储介质可以包括：U 盘、移动硬盘、只读存储器、随机存取存储器、磁碟或者光盘等各种可以存储程序代码的介质。

基于以上实施例，本申请实施例还提供了一种芯片。该芯片包括处理器，用于实现上述任意一个或多个实施例所涉及的功能，例如获取或处理上述方法中所涉及的第一报文。可选地，所述芯片还包括存储器，用于处理器所执行必要的程序指令和数据。该芯片，可以由芯片构成，也可以包含芯片和其他分立器件。

本申请是参照根据本申请实施例的方法、设备（系统）和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本申请实施例进行各种改动和变型而不脱离本申请实施例的范围。这样，倘若本申请实施例的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求 书

1. 一种无线局域网 WLAN 系统，其特征在于，包括接入控制器 AC、第一接入点 AP 和第二 AP，所述第一 AP 和第一站点 STA 关联，所述第二 AP 和第二 STA 关联，其中：

5 所述 AC 用于生成第一组临时密钥 GTK，向所述第一 AP 和所述第二 AP 发送第一 GTK；
所述 AP 用于通过所述第一 GTK 加密数据，得到第一报文，组播或广播所述第一报文；
所述 AP 用于向所述第一 STA 发送所述第一 GTK，所述第一 GTK 用于所述第一 STA 根据所述第一 GTK 解密所述第一报文；

10 所述 AP 用于向所述第二 STA 发送所述第一 GTK，所述第一 GTK 用于所述第二 STA 根据所述第一 GTK 解密所述第一报文。

2. 根据权利要求 1 所述的 WLAN 系统，其特征在于，

所述 AC 用于生成第一 GTK 包括：所述 AC 用于根据组主密钥 GMK、组随机数和所述 AC 的 MAC 地址生成所述第一 GTK。

15 3. 根据权利要求 2 所述的 WLAN 系统，其特征在于，所述 AC 用于向所述第一 AP 和所述第二 AP 发送第一 GTK 包括：所述 AC 用于向所述第一 AP 和所述第二 AP 发送第一消息，所述第一消息包括所述第一 GTK；

所述第一消息还包括以下至少一个：所述第一 AP 和所述第二 AP 的标识、所述第一 AP 中的虚拟接入点 VAP 的标识、所述第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、所述组随机数、完整性群组临时密钥。

20 4. 根据权利要求 2 或 3 所述的 WLAN 系统，其特征在于，所述 AC 还用于向所述第一 AP 和所述第二 AP 发送第一指示；

所述第一 AP 还用于根据所述第一指示关闭 GTK 的自动更新；

所述第二 AP 还用于根据所述第一指示关闭 GTK 的自动更新。

25 5. 根据权利要求 2 至 4 中任意一项所述的 WLAN 系统，其特征在于，当存在新的 AP 连接所述 AC 时，所述 AC 还用于向所述新的 AP 发送所述第一消息。

6. 根据权利要求 2 至 5 中任意一项所述的 WLAN 系统，其特征在于，当满足以下任意一项条件时，所述 AC 还用于向所述第一 AP 和所述第二 AP 发送更新后的第一 GTK；

所述条件包括：所述 AC 重启、所述 AC 中的密钥定时器超时、所述 AC 的加密模式从公开变为加密、使用所述第一 GTK 的 STA 离线。

30 7. 根据权利要求 6 所述的 WLAN 系统，其特征在于，

所述 AC 还用于根据更新后的 GMK、更新后的组随机数和所述 AC 的 MAC 地址更新所述第一 GTK，得到所述更新后的第一 GTK。

8. 根据权利要求 2 至 7 中任意一项所述的 WLAN 系统，其特征在于，所述 WLAN 系统还包括第三 AP；

35 所述 AC 还用于获取三个 AP 的分组参考信息，所述三个 AP 包括所述第一 AP、所述第二 AP 和所述第三 AP；

所述 AC 还用于根据所述分组参考信息确定所述第一 AP 和所述第二 AP 使用所述第一 GTK，所述第三 AP 使用第二 GTK，所述第二 GTK 和所述第一 GTK 不同。

9. 根据权利要求 8 所述的 WLAN 系统，其特征在于，

40 所述 AC 还用于向所述第三 AP 发送所述第二 GTK；

或,

所述 AC 还用于向所述第三 AP 发送控制指示;

所述第三 AP 用于根据所述控制指示生成所述第二 GTK。

10. 根据权利要求 8 或 9 所述的 WLAN 系统, 其特征在于, 所述分组参考信息包括 AP 之间的信道质量信息、所述三个 AP 所关联 STA 的位置信息或所述三个 AP 所关联 STA 的点播信息; 其中, 所述 AP 之间的信道质量信息包括所述三个 AP 中任意两个 AP 之间的信道质量信息。

11. 根据权利要求 1 至 10 中任意一项所述的 WLAN 系统, 其特征在于,

所述第二 STA 还用于从所述第二 AP 漫游至所述第一 AP;

所述第一 AP 还用于通过所述第一 GTK 加密数据, 得到第二报文, 组播或广播所述第二报文;

所述第二 STA 还用于根据所述第一 GTK 解密所述第二报文。

12. 根据权利要求 1 至 11 中任意一项所述的 WLAN 系统, 其特征在于, 所述第一 AP 和所述第二 AP 使用相同的基本服务集标识符 BSSID。

13. 根据权利要求 1 至 12 中任意一项所述的 WLAN 系统, 其特征在于, 所述第一报文为组播报文, 所述第一报文的目的地 IP 地址为第一组播组的 IP 地址;

当所述第一 STA 属于所述第一组播组时, 所述第一 STA 用于处理解密后的所述第一报文;

当所述第一 STA 不属于所述第一组播组时, 所述第一 STA 用于丢弃解密后的所述第一报文。

14. 根据权利要求 1 至 13 中任意一项所述的 WLAN 系统, 其特征在于, 所述第二 STA 与所述第一 AP 之间的信号质量信息大于第一阈值。

15. 一种无线通信方法, 其特征在于, 包括:

控制器 AC 生成第一组临时密钥 GTK,

所述 AC 向所述第一接入点 AP 和所述第二 AP 发送第一 GTK, 所述第一 GTK 用于第一站点 STA 和第二 STA 解密所述第一 AP 组播或广播的第一报文, 所述第一 AP 和所述第一 STA 关联, 所述第二 AP 和所述第二 STA 关联。

16. 根据权利要求 15 所述的方法, 其特征在于,

所述 AC 生成第一 GTK 包括: 所述 AC 根据组主密钥 GMK、组随机数和所述 AC 的 MAC 地址生成所述第一 GTK。

17. 根据权利要求 16 所述的方法, 其特征在于,

所述 AC 向所述第一 AP 和所述第二 AP 发送第一 GTK 包括: 所述 AC 向所述第一 AP 和所述第二 AP 发送第一消息, 所述第一消息包括所述第一 GTK;

所述第一消息还包括以下至少一个: 所述第一 AP 和所述第二 AP 的标识、所述第一 AP 中的虚拟接入点 VAP 的标识、所述第二 AP 中的 VAP 的标识、密钥重放计数器、接收顺序计数器、所述组随机数或完整性群组临时密钥。

18. 根据权利要求 15 至 17 中任意一项所述的方法, 其特征在于, 所述方法还包括:

所述 AC 向所述第一 AP 和所述第二 AP 发送第一指示, 所述第一指示用于所述第一 AP 和所述第二 AP 根据所述第一指示关闭 GTK 的自动更新。

19. 根据权利要求 15 至 18 中任意一项所述的方法, 其特征在于, 当满足以下任意一项条件时, 所述方法还包括:

所述 AC 向所述第一 AP 和所述第二 AP 发送更新后的第一 GTK;

所述条件包括: 所述 AC 重启、所述 AC 中的密钥定时器超时、所述 AC 的加密模式从公开变为加密、使用所述第一 GTK 的 STA 离线。

20. 根据权利要求 19 所述的方法, 其特征在于, 所述方法还包括:

所述 AC 根据更新后的 GMK、更新后的组随机数和所述 AC 的 MAC 地址更新所述第一 GTK, 得到所述更新后的第一 GTK。

21. 根据权利要求 15 至 20 中任意一项所述的方法, 其特征在于, 在所述 AC 向所述第一 AP 和所述第二 AP 发送第一消息之前, 所述方法还包括:

所述 AC 获取三个 AP 的分组参考信息, 所述三个 AP 包括所述第一 AP、所述第二 AP 和第三 AP;

所述 AC 根据所述分组参考信息确定所述第一 AP 和所述第二 AP 使用所述第一 GTK;

所述 AC 根据所述分组参考信息确定所述第三 AP 使用第二 GTK, 所述第二 GTK 和所述第一 GTK 不同。

22. 根据权利要求 21 所述的方法, 其特征在于, 在所述 AC 根据所述分组参考信息确定所述第三 AP 使用第二 GTK 之后, 所述方法还包括:

所述 AC 向所述第三 AP 发送所述第二 GTK;

或,

所述 AC 向所述第三 AP 发送控制指示, 所述控制指示用于所述第三 AP 根据所述控制指示生成所述第二 GTK。

23. 根据权利要求 21 或 22 所述的方法, 其特征在于, 所述分组参考信息包括 AP 之间的信道质量信息、所述三个 AP 所关联 STA 的位置信息或所述三个 AP 所关联 STA 的点播信息;

其中, 所述 AP 之间的信道质量信息包括所述三个 AP 中任意两个 AP 之间的信道质量信息。

24. 一种无线通信方法, 其特征在于, 包括:

第一接入点 AP 生成第一组临时密钥 GTK;

所述第一 AP 通过所述第一 GTK 加密数据, 得到第一报文;

所述第一 AP 组播或广播所述第一报文;

所述第一 AP 向第二 AP 和第一站点 STA 发送所述第一 GTK, 所述第一 GTK 用于所述第一 STA 根据所述第一 GTK 解密所述第一报文, 所述第一 AP 和所述第一 STA 关联, 所述第一 GTK 用于第二 STA 根据所述第一 GTK 解密所述第一报文, 所述第二 STA 和所述第二 AP 关联。

25. 一种无线通信装置, 其特征在于, 包括生成模块和发送模块, 其中:

所述生成模块用于生成第一组临时密钥 GTK;

所述发送模块用于向所述第一接入点 AP 和所述第二 AP 发送第一消息, 所述第一消息包括所述第一 GTK, 所述第一 GTK 用于第一站点 STA 和第二 STA 解密所述第一 AP 组播或广播的第一报文, 所述第一 AP 和所述第一 STA 关联, 所述第二 AP 和所述第二 STA 关联。

26. 一种无线通信装置, 其特征在于, 包括生成模块、加密模块和发送模块, 其中:

所述生成模块用于生成第一组临时密钥 GTK;

所述加密模块用于通过所述第一 GTK 加密数据, 得到第一报文;

所述发送模块用于组播或广播所述第一报文;

所述发送模块还用于向第二 AP 和第一站点 STA 发送所述第一 GTK, 所述第一 GTK 用于所述第一 STA 根据所述第一 GTK 解密所述第一报文, 所述装置和所述第一 STA 关联, 所述第一 GTK 用于第二 STA 根据所述第一 GTK 解密所述第一报文, 所述第二 STA 和所述第二 AP 关联。

27. 一种控制器 AC，其特征在于，包括处理器和收发器，其中：
- 所述处理器用于生成第一组临时密钥 GTK，
- 所述收发器用于向所述第一接入点 AP 和所述第二 AP 发送第一消息，所述第一消息包括所述第一 GTK，所述第一 GTK 用于第一站点 STA 和第二 STA 解密所述第一 AP 组播或广播的第一报文，所述第一 AP 和所述第一 STA 关联，所述第二 AP 和所述第二 STA 关联。
28. 一种第一接入点 AP，其特征在于，包括处理器和收发器，其中：
- 所述处理器用于生成第一组临时密钥 GTK；
- 所述处理器用于通过所述第一 GTK 加密数据，得到第一报文；
- 所述收发器用于组播或广播所述第一报文；
- 所述收发器还用于向第二 AP 和第一站点 STA 发送所述第一 GTK，所述第一 GTK 用于所述第一 STA 根据所述第一 GTK 解密所述第一报文，第一 AP 和所述第一 STA 关联，所述第一 GTK 用于第二 STA 根据所述第一 GTK 解密所述第一报文，所述第二 STA 和所述第二 AP 关联。